09/243,108 *

L3: Entry 61 of 97 File: USPT Mar 14, 2000

DOCUMENT-IDENTIFIER: US 6038551 A
TITLE: System and method for configuring and managing resources on a multi-purpose integrated circuit card using a personal computer

Abstract Text (1):
A computerized system offers a uniform platform for conducting electronic transactions in multiple different environments. The system includes a portable, multi-purpose, integrated circuit (IC) card and complimentary computer software which enables access and management of resources maintained on the IC card. The software runs on a user's personal computer, empowering the user to initialize the IC card, configure the card with the resources that the user wants to maintain on the card, and to manage those resources. The software enables the user to generate private/public key pairs and establish or change passcodes for access to the card resources. The IC card itself provides the electronic vehicle for securely transporting the user's private keys and certificates without exposing them in plaintext form. The IC card is designed with enough processing capabilities to perform rudimentary cryptographic functions so that the private keys may be employed for signing or encryption without ever being released from the card.

Brief Summary Text (2):
This invention relates to integrated circuit (IC) cards, such as smart cards, PC cards, and the like, which are capable of being used for multiple different applications. This invention further relates to systems and methods for initializing, configuring, and managing various resources maintained on the IC cards. This invention also relates to the secure management and transportation of cryptographic-related resources, such as keys and certificates, from one location to another.

Brief Summary Text (8):
Even outside of the commerce environment, the same themes of security, identification, authentication, and validity are becoming more important as reliance on computer networks increases. In modem network environments, identification and authentication are commonly used in access protocols aimed at preventing unauthorized users from gaining access to resources and services provided by the network. Typically, a user identifies himself or herself to a computer using a login dialog in which the user enters a descriptive and secret code name. The authentication process running on the computer validates the user based upon this confidential code name. Once validated, the user is free to roam the computer and network for resources and services. Unfortunately, the password authentication process often falls short of providing adequate security or user authentication. The password protocol, by itself, is well known to be weak and conducive to successful illegitimate attacks.

Brief Summary Text (9):
The problems inherent in password approaches has given rise to a variety of products which perform user authentication. Such products typically employ cryptographic technology in combination with hardware token devices. These token devices are typically pre-configured by the manufacturer and delivered to the user and replace the login password with a more robust and difficult to attack challenge-response protocol. While this technology is adequate for access control on an enterprise network (i.e., a local network for a business or other entity), it is not particularly scalable to public networks used by a large user population. This is

the result of reliance on a centralized access control server which has knowledge of all the tokens issued to valid users.

Brief Summary Text (10):
Another problem which existing hardware tokens has been generation and management of key values. "Keys" are a numerical value, often expressed digitally as a number of bits, which are used in cryptographic algorithms that encrypt and decrypt messages. The keys are uniquely associated with a particular identity, such as a user or a computer. Configuring millions of devices, each with its own unique keys, would be a huge processing task for the manufacturer, resulting in a significant increase in the cost of the hardware device. From a security standpoint, another problem is that the manufacturer becomes a centralized point of attack in which bandits can covertly attempt to steal private key information. Another problem concerns replacement of keys. Once a key has exhausted it useful life, the manufacturer must either issue new devices with new keys or reconfigure old devices to change the keys. Once again, this is an extremely difficult, expensive, and inefficient task in a large scale system.

Brief Summary Text (18):
Today, there are several electronic systems that provide cryptographic services in the computer forum. These include "Bsafe libraries" by RSA Data Security Inc., "X/Open CAPI", and "PKCS#". However, each of these systems permit direct access of the application to the keying material. There is no protection of these cryptographic resources from electronic attack. Furthermore, the Bsafe system, which is the most widely used cryptography system, directly attaches the cryptographic code to the application. There is no contemplation of protecting the keys from ignorant or malicious attacks from other software applications.

Brief Summary Text (24):
This invention provides a uniform platform for conducting electronic transactions in multiple different environments. The platform is based upon use of a portable, multi-purpose, integrated circuit (IC) card and complimentary computer software which enables user access and management of resources maintained on the IC card. The software runs on a user's personal computer, empowering the user to initialize the IC card, configure the card with the resources that the user wants to maintain on the card, and to manage those resources. The software enables the user to generate private/public key pairs and establish or change passcodes for access to the card resources. The IC card itself provides the electronic vehicle for securely transporting the user's private keys and certificates without exposing them in plaintext form. The IC card is designed with enough processing capabilities to perform rudimentary cryptographic functions so that the private keys may be employed for signing, encryption, and decryption without ever being exported from the card.

Brief Summary Text (26):
The system further includes various applications which execute on the computer, or more specifically, which run on the computer's operating system. For example, the applications might include a banking application, which is organizes the user's finances in conjunction with a particular bank; or an electronic commerce application, which allows the user to shop and purchase products over a public network; or a travel application, which permits the user to make vacation reservations; or an entertainment application, which enables the user to purchase tickets for entertainment events; or a gatekeeper application, which oversees access onto the network of the user's employer. In any one of these contexts, the application might require access to certain resources maintained on the IC card.

Brief Summary Text (27):
The system further includes an application interface which executes on the computer to implement each application and to provide services which facilitate access to the resources on the IC card that are requested by the application. The application interface is preferably implemented as a service layer for the operating system, and is securely integrated with the operating system via mutual authentication procedures. The application interface supports three distinct types of services. These include (1) configuration services which permit a user to initialize and configure the IC card with those resources tailored to the user's preferences, (2) security services which enable access to the cryptographic functionality on the IC

card, and (3) resource management services which permit the user to manage the storage provided by the IC card.

Brief Summary Text (28):
In one implementation, the application interface comprises a cryptographic services module and a card management services module. The cryptographic services module implements cryptographic functionality for the application. The cryptographic services module uses cryptographic resources maintained on the IC card and supplements this with software services. When the application requests a cryptographic function, the cryptographic services module communicates with the IC card to have the IC card support the cryptographic function. The IC card lends support without exposing the cryptographic resources maintained thereon. As an example, if the application requests a digital signature on a message, the application calls the cryptographic services module to hash the message to produce a digest and passes the message digest to the IC card. The IC card then digitally signs the digest using the user's private signing key and returns the signed digest to the application interface without exposing the signing key. The IC card can also assist in encryption, decryption, and authentication.

Brief Summary Text (29):
The card management services module implements the administration functionality for the application for managing resources maintained on the IC card. When the application requests performance of an administrative task on the IC card, the card management services module communicates with the IC card to perform the administrative task requested by the application. For example, the card management services module might support administrative tasks such as initialization of the IC card, generation of cryptographic keys, passcode configuration, and management of the IC card storage capabilities to hold certificates, and assets.

Brief Summary Text (30):
Another aspect of this invention is a card manager user interface (UI) which presents different graphical dialog screens to assist the user in managing her card resources. The card manager UI is very valuable from a usability standpoint. It provides a consistent presentation and method for managing the IC card resources which is independent of the applications being supported. The card manager UI allows the user to examine the resources of the card by using icon representations of the resources. The user can configure his/her card to add or remove resources simply by manipulating the graphical icons. The card manager UI also enables the user to initialize the IC card, and change passcodes for accessing the IC card.

Detailed Description Text (3):
FIG. 1 shows a computer system 10 having a computer 12 and a multipurpose integrated circuit (IC) card 14. The computer 12 includes a central processing unit (CPU) 16, a monitor or display 18, and a keyboard 20 (or other input device). The computer 12 is connected to a network 22 via a cable or wireless connection represented by line 24. The network 22 can be a data communications network including a wire-based network, such as an enterprise network (e.g., a local area network for a business) or a public network (e.g., the Internet), and a wireless network (e.g., satellite network). The network 22 can also be implemented as a telephone network, or an interactive television network, or any other form for linking the computer 12 to an external source of information.

Detailed Description Text (8):
The multi-purpose IC card 14 contains various resources that might be used by, or in support of, an application executing on the computer 12. Among these resources are cryptography capabilities. The IC card stores public and private key pairs and can hold related data such as public key certificates. The IC card also performs rudimentary cryptographic functions, including encryption, decryption, signing, authentication. The IC card may also contain resources in the form of electronic assets, which represent value. For instance, the IC card might store assets in the form of electronic entertainment tickets, travel reservations, service contracts, medical prescriptions, government entitlement provisions, electronic cash, public transportation tokens, and so on. With such diverse resources, the IC card 14 is capable of supporting multiple applications in different environments.

Detailed Description Text (10):
The multi-purpose IC card 14 provides a safe means for transporting the resources stored thereon. The IC card 14 can be physically ported with the user from place to place. The die design and fabrication processes used to manufacture the microcontroller IC yield a highly tamper-resistant card that is very difficult to reverse engineer and extract information. Thus, even if the card were lost or stolen, it is very difficult to obtain confidential information in the short time frame before the card is reported as lost and marked inactive. The IC card thus offers a secure storage and transportation mechanism for the cryptographic resources, and namely, the private keys.

Detailed Description Text (11):
The computer system 10 includes a software application interface which executes on the computer 12 to prevent possible covert attacks from malicious software applications which attempt to gain unauthorized access to resources on the IC card. The application interface implements the application and provides services which facilitate access to the resources on the IC card 14, without allowing the application itself to directly access the card-based resources. The application interface is implemented as a service layer for the operating system and is securely integrated with the operating system through mutual authentication. During initialization, the application interface and the operating system exchange certificates containing identifications (i.e., serial numbers or the like) which are signed by a trusted certifying authority (e.g., the manufacturer). The operating system and application interface then authenticate each other using the certificates. One technique for authenticating the various components in a computer system is described in a co-pending U.S. patent application Ser. No. 08/531,567, now U.S. Pat No. 5,221,781 filed Sep. 13, 1995, entitled "Authentication System and Method for Smart Card Transactions." This application is hereby incorporated by reference.

Detailed Description Text (14):
The multiple applications, referenced generally as number 34, run on the operating system at a high level, application layer. The API layer, referenced generally as number 36, resides between the application layer and the driver layer. The application interface 36 is a service layer which supports three distinct types of services: (1) configuration services which permit a user to reconfigure the IC card with those resources tailored to the user's preferences; (2) security services which enable access to the cryptographic functionality on the IC card; and (3) resource management services which permit the user to manage the resources provided by the IC card.

Detailed Description Text (15):
The API 36 includes a card management services module 38 and a cryptographic services module 40. The card management services module 38 implements administration functionality for the applications 34 for managing resources maintained on the IC card 14. When the application requests that an administrative task be performed on the IC card 14, the card management services module 38 communicates with the IC card to perform the administrative task. As an example, the administrative tasks include initialization of the IC card, cryptographic key generation, passcode configuration, management of cryptographic keys on the IC card, management of certificates on the IC card, and management of assets on the IC card. The interface presented to the user by the card management services module is consistent and application independent for usability. An example set of API calls is described below in more detail.

Detailed Description Text (16):
The cryptographic services module 40 implements cryptographic functionality for the application 34 while using cryptographic resources maintained on the IC card 14. When the application 34 requests a cryptographic function, the cryptographic services module 40 communicates with the IC card 14 and works cooperatively with the IC card 14 to perform the cryptographic function without exposing the cryptographic resources maintained on the IC card 14. As an example, the cryptographic services module 40 supports the following requests from the application: generating one or more cryptographic keys on the IC card, retrieving the public component of a public/private cryptographic key pair from the IC card, adding a certificate (or

other data resource) to the IC card, retrieving a certificate from the IC card, deleting a certificate from the IC card, generating a message digest based on an application supplied message, signing a message digest, encrypting data supplied by the application, decrypting data supplied by the application, verifying a signature supplied by the application, encrypting an encryption symmetric key for key exchange, decrypting a symmetric key supplied by the application. An example set of API calls is described below.

Detailed Description Text (20):
The CSP is preferably implemented in software as dynamic linked libraries (DLLs). This implementation is advantageous because it can be easily invoked by the CAPI or by the application through the CAPI. Furthermore, the cryptographic functions can be changed or updated simply by replacing one or more DLLs. With the CAPI layer in between, the CSP DLLs can be replaced without affecting how the application interacts with them. Additionally, by packaging the cryptographic services in DLLs, it will be possible to change the strengths of the services as regulatory considerations change without impacting the higher level application.

Detailed Description Text (22):
The IC card 14 stores and manages the cryptographic keys and associated data resources used by the CSP 44 in performing the cryptographic function. The IC card 14 can also perform rudimentary cryptographic functions in support of the CSP 44.

Detailed Description Text (30):
When an application 34 requests cryptographic functions, the IC card 14 works in cooperation with the CSP 44 to provide cryptographic functionality. The CSP performs most the of encryption and decryption processes which require greater computational resources. With present technology, IC cards in general cannot adequately perform full encryption/decryption of large size documents/messages due to I/O and processing limitations of the small microcontroller. However, the IC card can provide signatures and verification functions, and is capable of encrypting or decrypting small messages. As technology continues to evolve, it is expected that IC cards will have powerfull and fast processors that can satisfactorily encrypt messages of any size and sign them within the context of the desired environment without noticeable or irritating delay.

Detailed Description Text (31):
With continuing reference to FIG. 3, electronic assets 80 are also stored in the private segment of the EEPROM 56. These electronic assets represent value, and might include tickets, tokens, e-cash, service contracts, medical prescriptions, reservations, government entitlements, or a pointer to a source of value. Non-cryptographic programs 82 that the user might wish to load onto the IC card are kept in the EEPROM 56. These programs can be complimentary routines that assist the applications running on the computer to organize or manipulate data and assets on the card.

Detailed Description Text (32):
Unlike prior art IC cards and readers which are factory configured and offer limited, if any, customization by the user, the computer system 10 permits the user to extensively configure the IC card 14 according to his/her preferences after the card has been issued. As shown in FIG. 2, the computer system 10 has a card manager user interface (UI) 84 executing on the computer CPU at the application layer. The card manager UI 84 presents a uniform set of graphical dialog screens which enable the user to conveniently and easily manage the card resources (including cryptographic resources, assets, etc.) from the computer.

Detailed Description Text (35):
FIG. 5 shows an example resource management graphical screen 96 which is also part of the card manager pop-up box 90. The resource screen 96 provides a convenient interface that allows the user to manage the resources maintained on the card. The resource screen 96 presents a list 98 of resources that are presently stored on the user's IC card and a resource list 100 of available resources that can be added to the card. The icons represent various resources, such as parental control features 102, financial account access 104, entertainment-related assets 106, medical information 108, travel reservations 110, and telephone assets 112.

Detailed Description Text (36):
The user manipulates the icons to add assets to, or remove assets from, the IC card. This can be done using a conventional drag-and-drop protocol where the user clicks on the desired icon using a mouse or other pointing device, and drags the icon to the appropriate location. For instance, the user can drag the travel icon 110 from the resource list 100 to the card list 98 to add this resource to the card. In the illustrated example, a travel-relate asset (i.e., ticket reservations) has been added to the user's card. The IC card is thus equipped with travel accommodations and the user can port the IC card to the airport to download this travel asset when checking in for the flight. Other task-oriented input protocols, in addition to the drag-and-drop protocol, can be used to manage the resources on the IC card.

Detailed Description Text (37):
When the user manipulates the resources on the IC card, the card management services module 38 perfonns the actual card maintenance. For instance, to add a ticket-related asset, the card management services module 38 downloads the new "ticket" (i.e., application defined electronic representation of the ticket) to the IC card which is stored in the EEPROM. As another example, to add new cryptographic resources, the card management service module 38 might reconfigure the processing capabilities of the IC card by updating or changing a stored programs kept in memory the IC card read/write memory.

Detailed Description Text (40):
FIG. 6 shows an example illustration of how the IC card 14 is used for many different applications, while securely storing the resources on the card. In this example illustration, IC card 14 is configured with the user's medical information, financial data, work access account, tokens for beverage and snack vending machines, and various online service accounts including an electronic shopping account.

Detailed Description Text (41):
The user first inserts the IC card 14 into his/her home computer 120 for initialization and configuration using the card manager UI. Using the card manager UI, the user sets the IC card to an initial state in which the memory is cleared. The user then establishes one or more passcodes, which are stored on the IC card. Next, the user configures the IC card with certain resources to tailor the card to his/her preferences.

Detailed Description Text (45):
The user is free to spend the electronic cash on various goods and services, such as tokens for public transportation, food at a grocery store, and so on. As a further example, suppose the user decides to purchase a beverage from a vending machine 132. The user transports the same IC card 14 to the vending machine 132 and inserts it into a compatible card reader. The vending machine is an example of an offline computer, one that is not attached to a back end network. When the user selects the beverage, a vending machine application running on the vending machine requests through the API that the monetary equivalent of the cost of a beverage be withdrawn from the IC card 14. To access the private storage, the user might be requested to enter a passcode which is verified to the IC card. On the other hand, for such low cost items, there may be no need to verify the user via the passcode, or any other security protocol. The IC card 14 exports assets sufficient to pay for the beverage to the vending machine application, which then releases the beverage.

Detailed Description Text (46):
Now suppose on the way home, the user is injured and requires evaluation at a hospital 134. The IC card 14 can be accessed at the hospital to download the user's medical information from the public storage of the IC card's EEPROM. This can be done without requiring the user's passcode in the event the user is i unable to function due to the injury.

CLAIMS:

1. A system for supporting at least one computer-implemented application to access and manage a multi-purpose integrated circuit (IC) card, the system comprising:

a multi-purpose integrated circuit (IC) card having a plurality of resources for different uses;

a card reader which interfaces with the IC card to transfer information to and from the IC card;

a computers coupled to the card reader, to implement at least one application to enable a user to access and manage select resources of the plurality of resources of the IC card; and

an application-independent application interface executing on the computer to implement services utilized by the computer-implemented application to facilitate user access to certain of the plurality of resources provided by the IC card.

3. A system as recited in claim 1, wherein the application-independent application interface supports resource management services which permit a user to manage the resources provided by the IC card.

18. A computer-implemented application program interface to interface an application executing on a computer operating system with a program executing on an integrated circuit (IC) card, the IC card being coupled to communicate with a computer on which the operating system is running, the application program interface comprising:

a cryptographic services module which implements cryptographic functionality for the application, the cryptographic services module using cryptographic resources maintained on the IC card so that when the application requests a cryptographic function, the cryptographic services module communicates with the IC card to have the IC card support the cryptographic function without exposing the cryptographic resources maintained thereon; and

a card management services module which implements administration functionality for the application for managing resources maintained on the IC card so that when the application requests that an administrative task be performed on the IC card, the card management services module communicates with the IC card to perform the administrative task requested by the application.

21. A computer-implemented application program interface as recited in claim 18, wherein the cryptographic services module comprises:

a cryptographic application program interface (CAPI) to interface with the application and handle the application's request for the cryptographic function; and

a cryptography service provider (CSP) independent from, but dynamically accessible by, the CAPI, the CSP performing the cryptographic function requested by the application by accessing the IC card for support of the cryptographic function while protecting the cryptographic resources on the IC card to prevent exposure of the cryptographic resources to the CAPI and the application.

26. A computer to configure and manage a plurality of resources of an integrated circuit (IC) card, the computer comprising:

a processor;

a display; and

a card manager user interface (UI) executing on the processor, the card manager UI presenting at least one graphical dialog screen on the display which enables a user to reconfigure the IC card and to manage the resources on the IC card.

27. A computer as recited in claim 26, wherein the card manager UI has icons representing resources on the IC card.

28. A computer as recited in claim 27, wherein the card manager UI enables a user to add and delete resources by manipulating the icons presented on the graphical dialog

screen.

29. A computer as recited in claim 26, wherein:

the card manager UI presents a resource list of available resources that can be placed on the IC card; and

the card manager UI enables the user to add resources from the resource list to the IC card and to remove resources from the IC card to the resource list.

30. A configuration system enabling a user to configure an integrated circuit (IC) card after manufacture of the IC card, the IC card having a processor and programmable memory, the configuration system comprising:

a computer having a card reader to interface with the IC card; and

a card management application interface executing on the computer to enable the user to access the IC card and add, delete and otherwise configure the resources of the IC card stored within the programmable memory with data selected by a user.

31. A configuration system as recited in claim 30, wherein the card management application interface permits a user to manage resources on the IC card.

32. A configuration system as recited in claim 30, fuirther comprising a graphical user interface executing on the computer to present graphical representations of resources that are available on the IC card.

49. A method for personalizing contents on an integrated circuit (IC) card from a computer according to a user's preferences, the method comprising the following steps:

interfacing the IC card to the computer with an application-independent application interface executing on the computer;

presenting a user interface on the computer to the user as part of the execution of the application interface;

initializing the IC card using the user interface;

configuring the IC card, using the user interface, to include cryptographic resources and non-cryptographic resources; and

managing the cryptographic and non-cryptographic resources that are maintained on the IC card using the user interface.

50. A method as recited in claim 49, wherein the managing step comprises adding resources to, and removing resources from, the IC card.

51. A method as recited in claim 49, further comprising the following steps:

partitioning a memory on the IC card into a private storage and a public storage; and

the configuring step comprises storing some of the resources in the private storage and some of the resources in the public storage, and establishing a passcode for use in accessing the private storage.

52. A method for conducting secure electronic transactions comprising the following steps:

configuring, at a first computing site, a portable multi-purpose integrated circuit (IC) card with resources that enable the IC card to be used for multiple purposes, the resources including a cryptographic key and a certificate which can be used for at least one of the multiple purposes;

transporting the multi-purpose IC card from the first computing site to a second computing site;

interfacing the multi-purpose IC card with an application interface executing at the second computing site, the application interface supporting an application which is executing at the second computing site to process data for a designated purpose, the application requiring transformation of at least a portion of the data according to a cryptographic function, the application having a certificate;

exchanging certificates between the application and the IC card to verify authenticity to each other;

establishing data communication between the application and the IC card through the application interface;

supplying a request for the cryptographic function from the application to the application interface;

performing the cryptographic function cooperatively between the application interface and the IC card using the cryptographic key stored on the IC card without exposing the cryptographic key from the IC card;

transporting the IC card from the second computing site to a third computing site;

interfacing the IC card with an application interface executing at the third computing site, the application interface at the third computing site supporting an application which is executing at the third computing site and requires access to a non-cryptographic resource on the IC card for another designated purpose;

establishing data communication between the application and the IC card through the application interface;

making a request from the application for the non-cryptographic resource on the IC card; and

fulfilling the request for the non-cryptographic resource.